

In the Claims:

Cancel Claims 1-14 and add the following new Claims 15-47.

- 1 15. (New) A system for using a shared key to transmit secure data
2 between a client and a server, the system comprising:
3 an encrypt/decrypt engine for using the shared key to encrypt
4 or decrypt data, the encrypt/decrypt engine being
5 configured for delivery via a web page to a client in
6 response to a user request and further configured to
7 encrypt data independently of an identity of the physical
8 client;
9 wherein the server includes a user private keys database
10 configured to store the shared key. And, wherein, it is
11 possible for the client and the server to reside on the same
12 physical computing device. And when the shared key is
13 derived from the user's authentication data and the
14 derived shared key is used for encrypting all data.
- 1 16. (New) The system of claim 15 wherein the shared key is a user's
2 private key entered by a user into the web page.
- 1 17. (New) The system of claim 15 further comprising a secure data
2 database configured to store data received from the client and,
3 upon the completion of a processing step, to deliver the stored
4 data in an encrypted format to the client or to another client.

1 18. (New) The system of claim 15 further comprising a secure data
2 database configured to store data received from the client and,
3 upon receipt of a request for the data, to deliver the stored data
4 in an encrypted format to the client or to another client.

1 19. (New) The system of claim 15 wherein the shared key is
2 transmitted between the server and the client as few as zero
3 times and the shared key is transmitted between the server and
4 the user as few as one time. The key is not sent for
5 authentication purposes, rather, the effect of the key in the
6 encryption process is sent. Consequently, the shared key does
7 not need to be retransmitted once it has been established.

1 20. (New) The system of claim 15 wherein the shared key is a user's
2 private key entered by a user.

1 21. (New) The system of claim 15 wherein the client encrypt/decrypt
2 engine is installed on the client.

1 22. (New) A system for using a shared key in transmitting secure
2 data between a client and a server, the system comprising:
3 an encrypt/decrypt engine for using the shared key in
4 encrypting data, the encrypt/decrypt engine being
5 configured to encrypt data independently of an identity of
6 the client; and

7 a user private keys database located on the server and
8 configured to store the shared key, the shared key being
9 the private key of a user. And, when the shared key is
10 derived from the user's authentication data and the
11 derived shared key is used for encrypting all data.

1 23. (New) The system of claim 22 wherein the server is configured to
2 decrypt encrypted data received from the client using the shared
3 key and to use a private server key, known only by the server, to
4 re-encrypt the decrypted data.

1 24. (New) The system of claim 23 further comprising a secure data
2 database configured to store the encrypted data received from
3 the client and re-encrypted by the server and to deliver the
4 stored data to the client or to another client; the delivered data,
5 after the completion of a processing step, being encrypted with
6 the shared user key or with another shared user key. And, when
7 the shared key is derived from the user's authentication data
8 and the derived shared key is used for encrypting all data.

1 25. (New) The system of claim 23 further comprising a secure data
2 database configured to store the encrypted data received from
3 the client and re-encrypted by the server and to deliver the
4 stored data to the client or to another client; the delivered data
5 being, upon receipt of a request for the data, encrypted with the

{00060392v1}

6 shared user key or with another shared user key, when the
7 shared key is derived from the user's authentication data and
8 the derived shared key is used for encrypting all data..

1 26. (New) The system of claim 25 wherein the request is from the
2 user.

1 27. (New) The system of claim 25 wherein the request is from an
2 other user.

1 28. (New) A system for using a shared key in transmitting secure
2 data between a client and a server, the system comprising:
3 an encrypt/decrypt engine for using the shared key entered by a
4 user to encrypt data entered by the user, the
5 encrypt/decrypt engine being configured such that all
6 data entered by the user and stored on the client is stored
7 in encrypted form, and further configured to encrypt data
8 independently of an identity of the physical client; the
9 shared key entry being the responsibility of the user and
10 not the client;

{00060392v1}

11 the server including a user private keys database configured to
12 store the shared key, the shared key being a private key of
13 a user; and not a physical client and, when the shared
14 key is derived from the user's authentication data and the
15 derived shared key is used for encrypting all data.

1 29. (New) The system of claim 28, wherein the encrypt/decrypt
2 engine uses a symmetric key encryption/decryption algorithm
3 for encrypting and decrypting data.

1 30. (New) The system of claim 28, further including a web server
2 engine configured for the user to securely send or receive data
3 from the client to the server.

1 31. (New) A method for using a shared key in receiving secure data
2 on a server, comprising the steps of:
3 delivering from a server to a client a web page including an
4 encrypt/decrypt engine;
5 encrypting data on the client using the encrypt/decrypt engine
6 and a shared key entered by a user of the client, the
7 shared key being shared between the user and the server;

{00060392v1}

8 delivering the encrypted data from the client to the server; when
9 the shared key is derived from the user's authentication
10 data and the derived shared key is used for encrypting all
11 data;
12 receiving the encrypted data at the server;
13 decrypting the encrypted data at the server using the shared
14 key; and
15 processing the decrypted data, when the shared key is derived
16 from the user's authentication data and the derived shared key
17 is used for encrypting all data.

1 32. (New) The method of claim 31, wherein the step of processing the
2 decrypted data includes the steps of:
3 encrypting the decrypted data with a private server key; and
4 storing the encrypted data in a database.

1 33. (New) The method of claim 31, wherein the step of processing the
2 decrypted data includes the steps of:
3 re-encrypting the data with an other user's private key shared
4 between the other user and the server; and
5 sending the re-encrypted data to the other user.

1 34. (New) The method of claim 31, wherein the step of processing the
2 decrypted data includes the steps of:
3 decrypting the encrypted data with the private server key;

{00060392v1}

4 re-encrypting the data with a second user's key shared between
5 the second user and the server; and
6 sending the re-encrypted data to the second user.

1 35. (New) The method of claim 31, wherein the step of processing the
2 decrypted data includes the steps of:
3 processing the data according to an instruction of the user;
4 re-encrypting the processed data using the user's shared key;
5 and
6 sending the re-encrypted processed data to the user.

1 36. (New) The method of claim 31, wherein the step of processing the
2 decrypted data includes storing the decrypted data in a secure
3 database.

1 37. (New) A computer-readable medium comprising program
2 instructions for causing a computer system to use a shared key
3 in receiving secure data at a server, by the steps of:
4 delivering a web page from the server to a client, the web page
5 including an encrypt/decrypt engine and being configured

{00060392v1}

10

6 to use the encrypt/decrypt engine and a shared key
7 entered by a user of the client to encrypt data on the
8 client, the shared key being shared between the user and
9 the server;

10 receiving the encrypted data at the server;

11 decrypting the encrypted data using the shared key; and

12 processing the decrypted data and when the shared key is

13 derived from the user's authentication data and the derived

14 shared key is used for encrypting all data..

1 38. (New) A computer-readable medium comprising program

2 instructions for causing a computer system to receive secure

3 data on a server using a shared key, by the steps of:

4 delivering an encrypt/decrypt engine from the server to a client,

5 the encrypt/decrypt engine being configured to use a

6 shared key entered by a user of the client to encrypt data

7 on the client, the shared key being shared between the

8 user and the server and the encryption being independent

9 of an identity of the physical client;

10 receiving the encrypted data at the server;

11 decrypting the encrypted data using the shared key; and

12 processing the decrypted data, when the shared key is derived

13 from the user's authentication data and the derived shared key

14 is used for encrypting all data..

{00060392v1}

11

1 39. (New) The computer readable medium of claim 38, further
2 comprising program instructions for causing the processed
3 decrypted data to be re-encrypted using a private server key.

1 40. (New) The computer-readable medium of claim 39, further
2 comprising program instructions for causing the processed
3 decrypted data to be stored in a secure database.

1 41. (New) The computer-readable medium of claim 38, wherein
2 processing the decrypted data includes the steps of:
3 re-encrypting the data with the private server key;
4 storing the re-encrypted data;
5 decrypting the stored data with the private server key;
6 encrypting the data with a second user's key shared between
7 the second user and the server; and
8 sending the encrypted data to the second user.

1 42. (New) The computer-readable medium of claim 38, wherein
2 processing the decrypted data includes the steps of:
3 processing the data according to an instruction of the user;
4 encrypting the processed data using a shared key; and
5 sending the encrypted processed data to the user or to another
6 user.

1 43. (New) A method of using a shared key in transmitting secure data
2 between a client and a server using a shared key, comprising
3 the steps of:
4 encrypting data using the shared key with an encrypt/decrypt
5 engine configured to encrypt data independently of an
6 identity of the client, the shared key being entered by a
7 user of the client;
8 delivering the encrypted data from the client to the server;
9 receiving the encrypted data at the server;
10 decrypting the encrypted data at the server using the shared
11 key, the shared key being stored in a user private keys
12 database; and
13 processing the decrypted data, when the shared key is derived
14 from the user's authentication data and the derived
15 shared key is used for encrypting all data..

1 44. (New) The method of claim 43, wherein processing the decrypted
2 data includes the steps of:
3 encrypting the decrypted data with a private server key; and
4 storing the encrypted data in a database.

1 45. (New) The method of claim 43, wherein the step of processing the
2 decrypted data includes the steps of:
3 encrypting the data with an other user's private key shared
4 between the other user and the server; and

5 sending the encrypted data to the other user.

1 46. (New) The method of claim 43, wherein the step of processing the
2 decrypted data includes the steps of:
3 decrypting the re-encrypted data with the private server key;
4 encrypting the data with a second user's key shared between
5 the second user and the server; and
6 sending the encrypted data to the second user.

{00060392v1}

14